

## Internet Banking

# Protect your money with TWO-FACTOR AUTHENTICATION



## TWO-FACTOR AUTHENTICATION Stronger Security

Two-factor authentication protects you from Internet banking fraud. Take a few seconds to read how you can benefit from this new technology and enjoy far more secure online banking services. It is simple and straightforward. Contact your bank for more information about two-factor authentication.

Two-factor authentication is required if you wish to conduct high-risk Internet banking transactions.

### THE NEED FOR MORE THAN JUST A USER ID AND A PASSWORD

Cases have been reported of user IDs and passwords being stolen by fraudsters through phishing emails, fake websites, Trojan software and other malicious programmes. This shows the need to increase the security of Internet banking.

### TWO-FACTOR AUTHENTICATION

Two-factor authentication uses a combination of two different factors for verifying a user's identity.



e.g. user ID and password



e.g. digital certificate,  
security token or mobile phone

### THE BENEFITS OF USING TWO-FACTOR AUTHENTICATION

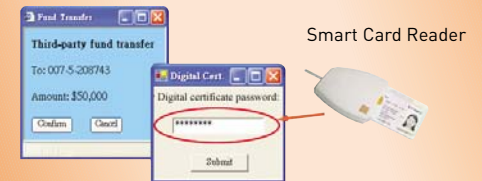
- **Much more secure** - fraudsters cannot steal 'something you have' in your physical possession (such as a mobile phone) over the Internet.
- **Protection for high-risk transactions** - all high-risk Internet banking transactions (such as fund transfers to non-designated accounts) are protected by an additional authentication factor which is physically held by you only.
- **Convenient and easy to use** - you can have substantially stronger online security by taking a few more steps, which are simple and straightforward.

Different banks may offer different types of two-factor authentication methods to customers. Three common types being adopted by banks are:

### Digital Certificate

An electronic identification certificate that helps establish your identity online. It can be stored in a smart card (e.g. the Hong Kong Smart ID card) or an electronic key (e.g. USB key).

- **How it works** You insert the smart card or key into a smart card reader or a USB port of a PC during the authentication process.

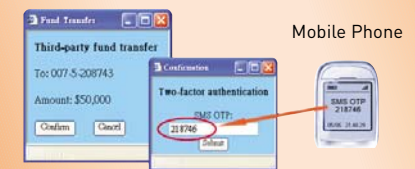


User inserts Hong Kong Smart ID card into a smart card reader and types in digital certificate password to confirm high-risk transaction

### SMS-based OTP

An SMS-based one-time password (OTP) generated by the bank and sent to your mobile phone for additional identity authentication. Each SMS OTP is used only once and expires within a short period of time.

- **How it works** When you initiate a high-risk transaction, you will receive an SMS OTP on your mobile phone. You then type in the OTP to confirm the transaction.



User types in SMS OTP to confirm high-risk transaction

## Security Token-based OTP

An OTP generated by a security device/token. Each OTP is used only once and expires within a short period of time.

- **How it works** You press the button on the security device/token to obtain an OTP, which is used as the additional identity authentication, e.g. to confirm a high-risk transaction.



User types in token-based OTP to confirm high-risk transaction

## REMEMBER

- Safeguard your device for two-factor authentication (e.g. smart card, security token or mobile phone).
- Follow the security tips given by your bank.

## MORE SAFETY TIPS

To protect your computer from unauthorised access or viruses, you should install the following software:

- **Personal firewall** to prevent hackers from getting into your computer. This allows you to control the information that passes between your computer and the Internet. It helps to block suspicious access to your computer over the Internet.
- **Anti-virus software** to prevent viruses from infecting your computer. Update your anti-virus software regularly to detect new viruses and do not download software from sources you do not trust.
- **Anti-spyware software** to prevent spyware from collecting your sensitive data. Update your anti-spyware software regularly to detect new spyware. To avoid being infected by spyware, do not download software from sources you do not trust.

## MORE INFORMATION

- If you have any questions about Internet banking, please contact your bank.

## USEFUL LINKS

Hong Kong Association of Banks

[www.hkab.org.hk](http://www.hkab.org.hk)

Hong Kong Monetary Authority

[www.hkma.gov.hk](http://www.hkma.gov.hk)

Hong Kong Police Force

[www.info.gov.hk/police/hkp-home/english/tcd/index.htm](http://www.info.gov.hk/police/hkp-home/english/tcd/index.htm)

INFOSEC, Office of the Government

Chief Information Officer

[www.infosec.gov.hk/english/general/protect/index.htm](http://www.infosec.gov.hk/english/general/protect/index.htm)

Consumer Council

[www.consumer.org.hk](http://www.consumer.org.hk)



HONG KONG MONETARY AUTHORITY

香港金融管理局



消費者委員會

CONSUMER COUNCIL

Issued by the Hong Kong Association of Banks and endorsed by the Hong Kong Monetary Authority, the Hong Kong Police Force and the Consumer Council.

May 2005